Combating Terrorism

Lieutenant Colonel Andrew J. Smith, Australian Army

ON 11 SEPTEMBER 2001, the United States was subjected to a complex, coordinated, devastating terrorist attack. In less than 2 hours, New York's World Trade Center and a portion of the Pentagon were destroyed, and four commercial airliners were lost with all passengers and crew.[1]

The full national and international response to this attack continues to take shape. Assessing the attack's physical consequences in terms of damage and casualties will take years.[2] On the international front, the United States has declared war on terrorism, and President George W. Bush has clearly defined the national strategic objective as eliminating terrorist groups "with global reach."[3] An antiterrorist coalition has commenced offensive operations against the perpetrators and their allies, and that coalition is sending a consistent message that the fight against terrorism will be long, costly, and difficult. While military action is under way abroad, the Bush administration has expanded the Cabinet to include a new portfolio for homeland security, and additional resources have been committed to improving security measures and intelligence capabilities that address terrorism. Other countries are also reassessing their arrangements for countering terrorism.[4]

This response suggests that Bush's mission to eradicate international terrorism will require a comprehensive set of countermeasures to address every aspect of that threat before, during, and after an attack. This article proposes a framework to evaluate the completeness of any strategy for combating generic terrorist attacks. The framework divides terrorists' offensive efforts and the counterterrorist response into preparatory, crisis, and consequence phases, each involving a particular set of terrorist activities that demand specific countermeasures.

Trends in Terrorism

Although the term "terrorist" dates from the late 18th century, terrorism has been used for thousands of years.[5] For most of its history, until the late 1960s, terrorism has been connected with insurgencies—a nonruling group's attempt to influence or overthrow a ruling group within a country or region.[6]

Civilian emergency services, such as fire brigades, ambulance services, and public health and law enforcement agencies, will assume their normal roles [during CBRNE attacks] but will often require a surge capacity to which military forces . . . may need to contribute. A smooth transition to large-scale consequence management operations will require frequent rehearsal in peacetime.

From the late 1960s, terrorist activities began to spread beyond the immediate boundaries of countries or regions in conflict. The increased mobility that much of the world's population experienced after World War II was probably the major contributing factor to this trend. Aircraft hijackings, in particular, became a terrorist technique with great ability to globalize terrorism. During the first three decades of the global terrorist period, terrorist techniques tended to limit physical damage or casualties.[7] Bombings—terrorists' historical technique of choice—tended to have limited effects because of the size of the devices that terrorists were able to assemble and transport.[8] Similarly, attacks using small arms tended to produce too few casualties.

One dangerous terrorist tactic employed several times during the 1970s and early 1980s was the hostage-siege. The Black September attack on the 1972 Munich Olympics is a good example of this tactic. The tactic was also frequently associated with aircraft hijackings. The hostage-siege focused world attention on the crisis phase of a terrorist operation and demonstrated that terrorists appreciate the value of international media and information operations (IO) in furthering their causes. This link between terrorist aims and hostage-siege tactics was

demonstrated by hijackings, which usually sought the release of political prisoners in exchange for hostages. Negotiation was sometimes a viable government option in resolving these crises because the terrorists' demands were affordable, however undesirable it may have been to concede to criminals. For most Western nations, the ultimate response to the hijacking threat was the development of sophisticated specialist capabilities for resolving hostage-siege crises by force. These were supported by passive methods such as inspecting luggage at airports. By the late 1980s, this effort had largely blunted the hostage-siege threat.[9]

"Counterterrorism," as defined in U.S . doctrine, refers to offensive measures usually involving lethal force taken directly against terrorist operatives and their activities. The best example of this connotation of counterterrorism is the employment of special recovery tactics to resolve hostage-siege situations.

Beginning in the early 1980s and developing through the 1990s, a disturbing new trend emerged in the motivation of the most dangerous terrorist groups. This was a shift toward more purely religious bases for their causes, accompanied by a tendency to demonize or dehumanize groups or societies they opposed. These factors enabled terrorists to justify methods capable of generating much larger numbers of casualties.[10] This was evident in the 1983 suicide truck-bomb attack on a U.S. Marine facility in Beirut, Lebanon, and in the 1984 bombing of the United Kingdom Conservative Party convention in Brighton, England. This trend gathered momentum during the 1990s.[11] Perhaps the most disturbing demonstration of mass destruction terrorism before 11 September was the Aum Shinrikyo (Aleph) sect's 1995 chemical nerve agent attack on the Tokyo subway system.

Another implication of the more religiously or ideologically based terrorist motivations of the 1990s was a trend toward a Huntingtonesque clash of civilizations approach; this trend was demonstrated by the jihadism of extremist Islamic groups such as Osama bin Laden's al-Qaeda network.[12] This may be a secondary reason for the demise of the hostage-siege tactic: terrorists' demands for civilizational change, such as "end global capitalism" or "terminate Western hegemony," cannot be physically granted or philosophically conceded by governments. Negotiation is therefore impossible.[13]

As with the hostage-siege phenomenon of the 1970s and 1980s, many countries have responded to the threat of mass destruction terrorism by developing dedicated capabilities to counter it. These include measures aimed at the crisis phase of a weapon of mass destruction or high-yield conventional explosive incident, as well as consequence management capabilities to mitigate the damage inflicted by a successful attack.[14]

Countering Terrorism

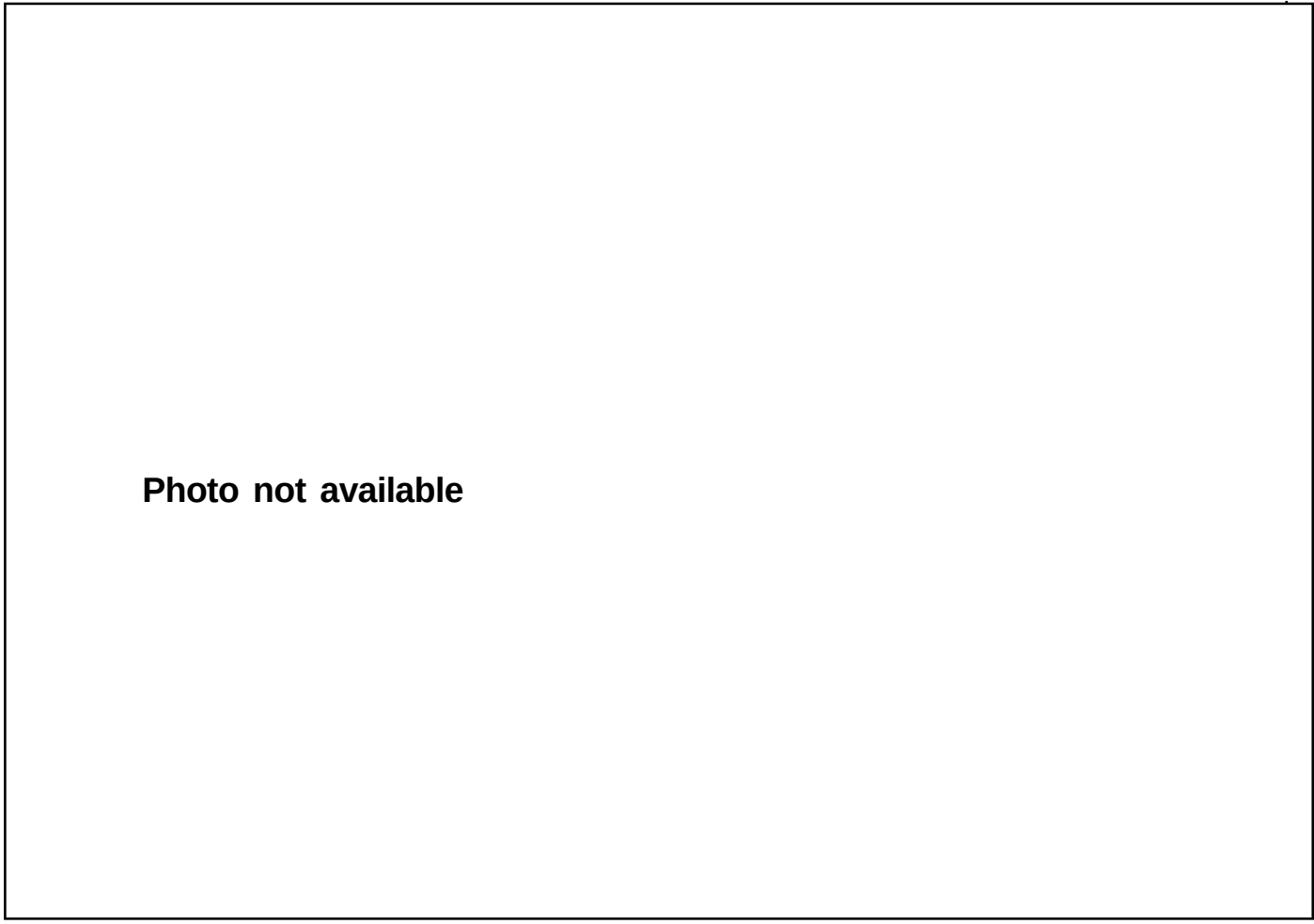
International terrorism has been a source of concern to governments for more than 30 years. Over that period, governments have developed a range of responses or countermeasures that have evolved into a distinct body of theory. In some cases, this theory extends to specific operational capabilities. Before proceeding to an analysis of terrorist attacks, it is useful to define at least the key concepts underpinning this body of theory.

"Terrorism" is a loosely defined term that is generally associated with politically motivated violence inflicted by nonstate groups, with or without state sponsorship. Measures designed to deal with terrorism are conventionally parsed into several categories. In U.S. doctrine, these measures are grouped under the collective term "combating terrorism." Within the scope of combating terrorism, activities are further divided into two categories: counterterrorism and antiterrorism. Other countries recognize this general distinction although the terminology used to refer to each category sometimes differs.[15]

"Counterterrorism," as defined in U.S. doctrine, refers to offensive measures usually involving lethal force taken directly against terrorist operatives and their activities. The best example of this connotation of counterterrorism is the employment of special recovery tactics to resolve hostage-siege situations. Because of its association with elite law enforcement or military capabilities, counterterrorism has taken on a secretive and compartmentalized dimension that may ultimately hinder efforts to develop a comprehensive government response to terrorism.[16]

"Antiterrorism" refers to passive or defensive measures taken to thwart a terrorist attack. These measures are extremely diverse and include such activities as physical security measures, bomb search and render safe capabilities, facility access control, and blast-hardening of structures.

"Consequence management" is a term that emerged in U.S. terrorism jargon during the late 1990s and refers to all measures used to mitigate the effects of terrorist attacks, particularly attacks involving chemical, biological, radiological, nuclear, or high-yield explosives (CBRNE).[17]



One dangerous terrorist tactic employed . . . during the 1970s and early 1980s was the hostage-siege. The Black September attack on the 1972 Munich Olympics is a good example of this tactic. The tactic was also frequently associated with aircraft hijackings. The hostage-siege focused world attention on the crisis phase of a terrorist operation and demonstrated that terrorists appreciate the value of international media and information operations in furthering their causes.

The Shape of Terrorist Attacks

The events of 11 September suggest that the crisis phase of a terrorist attack is too fleeting to rely on crisis management capabilities alone. The 11 September crisis was over in 2 hours, during which U.S. crisis management options were limited to shooting down the airliners. Subsequent actions in New York, rural Pennsylvania, and at the Pentagon amounted to consequence management, while other national and international activities were devoted to preventing the next attack. If 11 September demonstrates a trend toward increasingly lethal terrorist tactics, there are significant implications for how nations address this threat. Two areas of special concern are:

The possibility that the destruction achieved on 11 September has recalibrated terrorist actions, opening the possibility that follow-on attacks will aim for similar casualty levels.

The likelihood of terrorists being prepared for and surviving a destructive coalition response to their actions. This suggests that a second terrorist strike will be planned and ready for execution at the most advantageous time—after an apparently conclusive government counterstrike.

If the world is on the brink of an era of mass destruction terrorism, the experience of the past decade suggests two apparently contradictory imperatives in combating that type of terrorism:

Forestall terrorist efforts before they coalesce into a crisis because once a crisis emerges, it may be impossible to avoid devastating consequences. This compels a need for proactive countermeasures to prevent terrorist attacks.

Anticipate that terrorists—an increasingly adaptive enemy—will defeat the United States' preventive measures at least part of the time.[18] This makes it essential to maintain effective crisis and consequence management capabilities.

These conclusions suggest the need for a comprehensive suite of capabilities and efforts that can be brought to bear at any point in the evolution of an attack.

The 11 September attack illustrates that terrorist

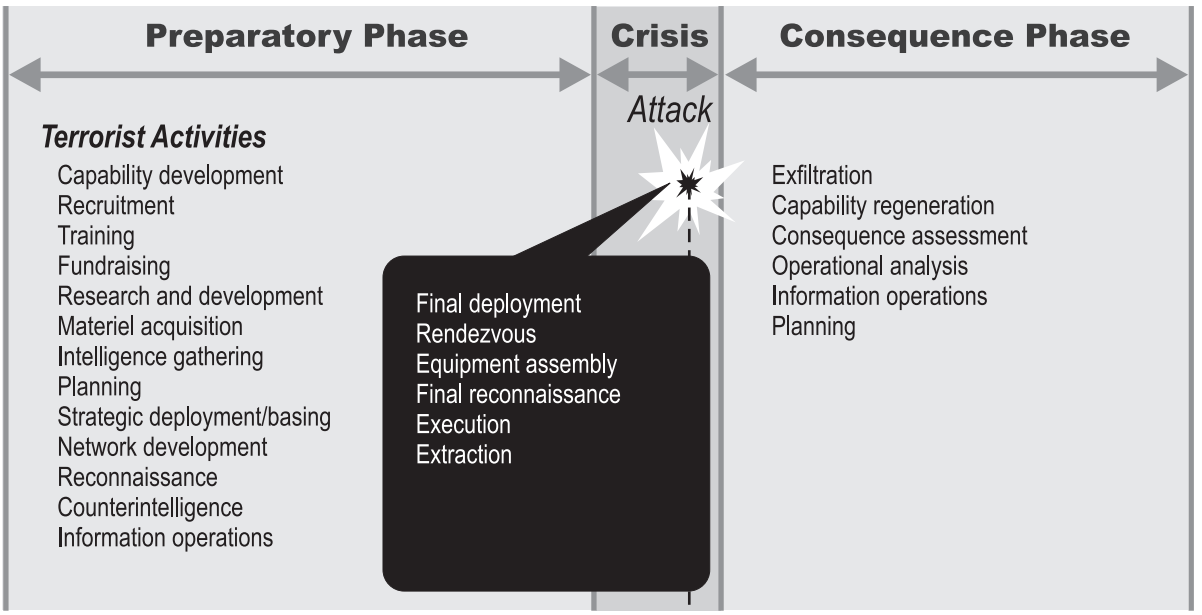


Figure 1. Generic Terrorist Activities Time Line

A typical global terrorist attack consists of a years-long preparatory phase, a very brief crisis phase, and a long consequence phase. The same timeline could apply to a terrorist campaign in which a number of attacks are made using a range of tactics. In such a case, the crisis phase could be drawn out, with attacks and their consequences overlapping.

groups are developing novel and devastating methods. Lengthy preparatory phases have preceded several of the more devastating attacks of the past 10 years.[19] During these phases, new capabilities were developed, operatives were recruited and trained, resources were positioned, and the attack was researched and planned.[20]

In contrast to the preparatory phase, the terrorists' actions on 11 September coalesced into the crisis phase very quickly. Final deployment for and execution of the attack all took place within a few hours. As the events of that morning demonstrate, the U.S. government was unable to react in time to prevent the terrorists from pressing home attacks against their targets.[21]

Consequences were generated even before the last of the four aircraft had crashed. Recovery efforts at the World Trade Center site are predicted to continue for several months. Significantly, the 11 September attacks were essentially conventional explosive incidents that generated mostly prompt casualties.[22] In a successful, large-scale CBRNE attack, a massive decontamination effort would be required, and delayed casualties would continue to present over a long period. A consequence management phase of two or more years is therefore realistic for a large-scale CBRNE incident.

This brief analysis suggests that a typical global terrorist attack consists of a years-long preparatory phase, a very brief crisis phase, and a long consequence phase. The same timeline could apply to a terrorist campaign in which a number of attacks are made using a range of tactics. In such a case, the crisis phase could be drawn out, with attacks and their consequences overlapping.

Using a generic model, the terrorists' activities throughout the evolution of their attack can be posted against the model. Represented graphically, their activities could look like Figure 1. If countermeasures are then arrayed against these terrorist activities, a comprehensive suite of measures and capabilities emerges as seen in Figure 2.

Comprehensive Countermeasures

Using this model, it is possible to compare terrorist activities in each phase with corresponding government countermeasures to determine whether gaps exist in the counterterrorist strategy.

During the capability development or preparatory phase, terrorist activities will be low profile and often difficult to link with deliberate hostile intentions. Countermeasures during this phase will focus on intelligence gathering and surveillance aimed at detecting terrorist groups and determining their motivation and intent. These efforts may also

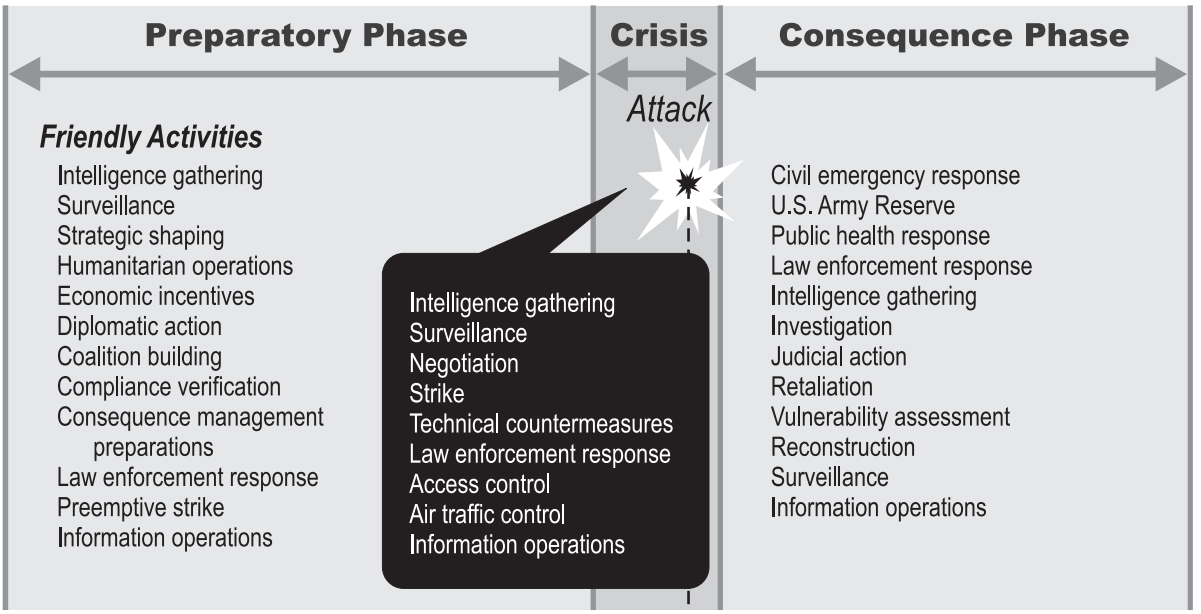


Figure 2. Generic Terrorist Countermeasures

detect terrorist-related criminal activities such as drug trading. Intelligence gathering may eventually lead to preemptive strikes against concentrations of terrorist activity or capabilities although these opportunities could be rare.[23] Intelligence efforts may also detect emerging terrorist tactics or capabilities, enabling the anticipatory development of new crisis and consequence management capabilities.[24] Selectively using IO to allow terrorists to learn of defensive preparations, without compromising operational security, could also deter terrorist acts.

The above measures are largely reactive and, except for preemptive strikes, cede the initiative to the terrorist. There are, however, proactive countermeasures available to governments during the preparatory phase. These could fall into two classes: direct and indirect. Direct countermeasures would consist mainly of law enforcement and military activities, such as intelligence gathering, and when possible, strike operations using air power or special operations assets.

Indirect countermeasures would consist of programs aimed at addressing the antipathies that motivate terrorists' actions.[25] For example, humanitarian aid programs should be synchronized with other diplomatic and economic initiatives to deprive the terrorists of a recruiting base of aggrieved persons. These measures would operate through diplomatic or economic means but their ultimate purpose would be informational.

Indirect countermeasures seek to shape the strategic environment in which the terrorist war is fought, but these countermeasures are difficult to aim at specific terrorist activity and are long-term in nature. The countermeasures should be in place before the terrorists form their intent to attack and should continue throughout the crisis and consequence phases. This suggests that the model might be refined by depicting indirect countermeasures as a permanent feature of a counterterrorist campaign, active through all phases of a particular incident.

Countermeasures during [the preparatory] phase will focus on intelligence gathering and surveillance . . . [which] may eventually lead to preemptive strikes. . . . [Such] measures are largely reactive and, except for preemptive strikes, cede the initiative to the terrorist. There are, however, proactive countermeasures available. . . . For example, humanitarian aid programs should be synchronized with other diplomatic and economic initiatives to deprive the terrorists of a recruiting base of aggrieved persons.

As indicated earlier, there may be limited opportunity to apply countermeasures during the crisis phase of an attack; the growing sophistication of the most dangerous terrorist groups and their increasing use of suicide tactics suggest that these opportunities are becoming increasingly rare. Nevertheless, crisis management capabilities are still necessary because they ease the transition to consequence management and bolster public confidence that the government is handling the crisis

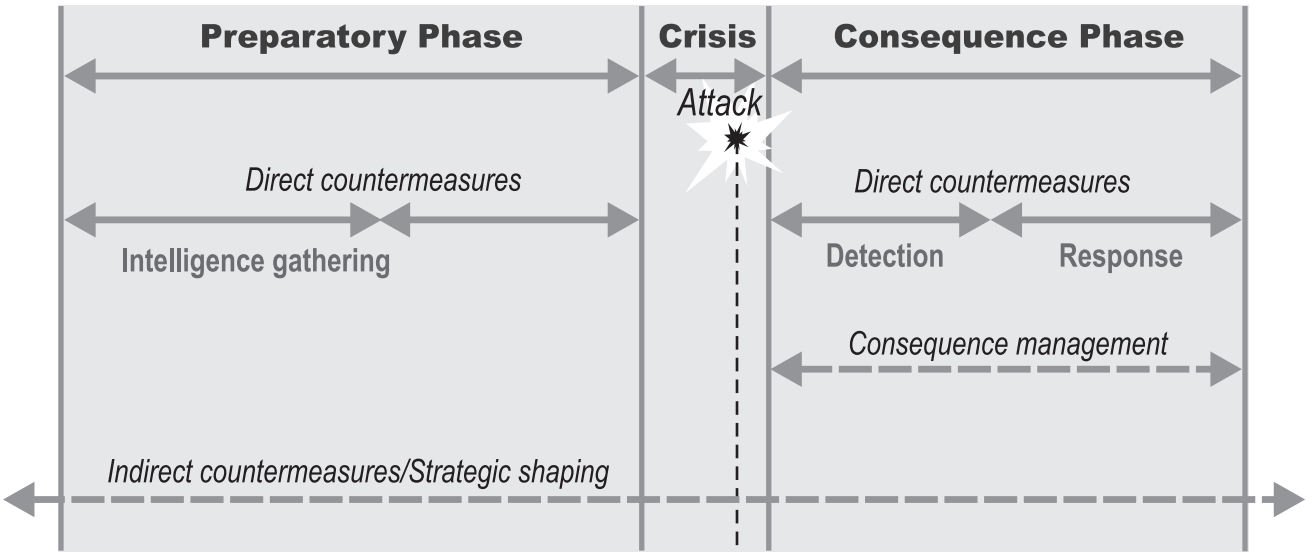


Figure 3. Refined Generic Model

The direct countermeasures applied during the consequence phase suggest further refinement of the generic model by dividing the consequence phase into two subphases: detecting and apprehending the perpetrators, and deliberate responses such as military retribution and the judicial trial of any arrested terrorists. This branch of government activity during the consequence phase thus aligns with much activity during the preparatory phase, forming a cycle of countermeasures.

competently. If successfully applied, crisis management capabilities may also mitigate or even avert serious physical consequences. It may be possible to maintain crisis management capabilities, such as special recovery assets for hostage-siege situations, by adapting these from the specialist operations capabilities needed for strategic strikes. As in the preparatory phase, aggressive and well-coordinated IO will be essential to government success during an attack's crisis phase.

Historically, crisis management has emphasized traditional counterterrorist capabilities and extensive command and control arrangements reaching to the national political level. The CBRNE dimension demands an expanded range of response capabilities such as bomb search and render safe; chemical, biological, and radiological agent detection and identification; and casualty handling. These highly specialized and demanding fields are beyond the reach of local governments and highlight the need for a national capability.

During the consequence phase of an attack, terrorists' efforts will be devoted to exfiltrating survivors, strategic and tactical repositioning for follow-on operations, exploiting any informational advantage, and evaluating the operation. Government activities during the consequence phase will necessarily concentrate initially on relief and recovery efforts. During CBRNE attacks, the scale of casualties, damage, and disruption can be reduced by effective and timely consequence management. Civilian emergency services, such as fire brigades, ambulance services, and public health and law enforcement agencies, will assume their normal roles but will often require a surge capacity to which military forces or other resources may need to contribute. A smooth transition to large-scale consequence management operations will require frequent rehearsal in peacetime.

During consequence management, other government efforts will be devoted to direct countermeasures similar to those applied during the preparatory phase. These will include meeting law enforcement challenges, including investigating the attack and arresting or detaining suspects. The government will also mount military, diplomatic, economic, and judicial responses. Early intelligence efforts should be devoted to determining if the attack is part of a coordinated campaign, cueing preemptive strikes, or adopting additional protective measures. Analyzing terrorist tactics can help develop new protective and consequence management techniques to reduce vulnerability in the future.

The direct countermeasures applied during the consequence phase suggest further refinement of the generic model by dividing the consequence phase

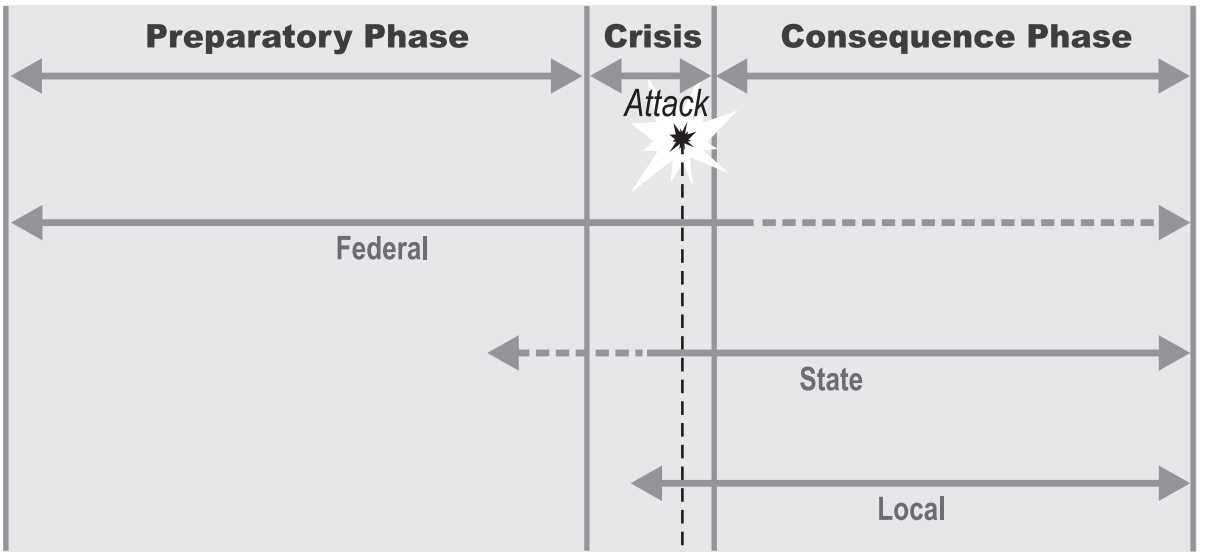


Figure 4. Terrorism Countermeasures by Government Level

into two subphases: detecting and apprehending the perpetrators, and deliberate responses such as military retribution and the judicial trial of any arrested terrorists. This branch of government activity during the consequence phase thus aligns with much activity during the preparatory phase, forming a cycle of countermeasures. IO must continue, aimed at restoring public morale and confidence and at mitigating any informational advantage the terrorists may have earned. If these refinements are incorporated into the model, the result could look like Figure 3.

Planning a Government Response

The preceding analysis shows that an extensive range of countermeasures must be available if any country is to have a comprehensive answer to the threat of modern terrorism. The generic model proposed also has some value in mapping the source of these capabilities in a federal model of government as exists in the United States, Australia, and many other Western nations.

Federal states tend to divide the responsibility for providing government services among different levels of government. Typically, these are the federal, state or provincial, and local or municipal levels. Federal responsibilities emphasize matters that impinge on national prosperity and security such as economic, foreign, and defense policy. State and local governments usually handle matters that more directly affect individual health and well-being such as law enforcement, education, health, and emergency services. All levels of government, therefore, command resources and capabilities that are relevant to countering terrorism. If the sources of these capabilities are arrayed against our generic model, the result could look like Figure 4.

Federal resources apply across the entire attack timeline, while state and local resources apply more to the crisis and consequence phases. For at least part of the crisis and consequence phases, resources commanded by all three levels of government play a role.

As this representation demonstrates, federal resources apply across the entire attack timeline, while state and local resources apply more to the crisis and consequence phases. For at least part of the crisis and consequence phases, resources commanded by all three levels of government play a role. This suggests that during these phases, there may be duplicated efforts and, perhaps more dangerously, jurisdictional conflicts which could hinder the most efficient and harmonious application of resources.[26] The exigencies of a war on terrorism may justify the abrogation of certain state and local government jurisdictions in favor of more efficient federal management. Significantly, traditional military forces are limited in their application right across the model.

Waging war on terrorism poses significant challenges for governments. Perhaps the greatest challenge lies in the range and complexity of countermeasures that must be developed and implemented to execute a truly comprehensive strategy. Successfully executing such a strategy will require a degree of coordination and planning that has heretofore eluded most Western nations, especially those that

Indirect countermeasures . . . are difficult to aim at specific terrorist activity and are long-term in nature. [They] should be in place before the terrorists form their intent to attack and should continue throughout the crisis and consequence phases. . . . indirect countermeasures [may be considered] a permanent feature of a counterterrorist campaign, active through all phases of a particular incident.

have a federal government system. The high level of management needed for efficient and robust countermeasures may necessitate a centralized approach to planning and execution. This may, in turn, necessitate that some intrastate jurisdictions sacrifice their traditional autonomy.

This article proposes a model for mapping elements of terrorist threats and corresponding countermeasures to gauge the comprehensiveness of any putative strategy for combating terrorism. Like the Cold War that preceded it, the impending war on terrorism promises to be a long one that will provide ample opportunity to test the validity of this model or any other construct that seeks to organize governments' efforts in the emerging international security environment. ***MR***

NOTES

1. "Timeline: Chronology of Events," 11 September 2001, <http://www.msnbc.com/news/631782.asp>.
2. Norma Cohen, "Debate on Future of WTC Site," *Financial Times*, (20 September 2001). <http://specials.ft.com/aoa/FT3F7IUWURC.html>.
3. President George W. Bush's address to the combined Houses of the U.S. Congress, 20 September 2001.
4. For example, Australia has declared that it will double its conventional counterterrorist capabilities and will reestablish special capabilities generated for the Sydney 2000 games. The Honorable Peter Reith, Member of Parliament, Minister for Defence Media Release, 2 October 2001.
5. Although the intent and methods of terrorism can be perceived in the activities of the Hebrew zealots of Roman times, the term itself is traceable in English to 1795 in the context of the French Revolution's Reign of Terror, *Oxford English Dictionary*. A link between anarchism and terrorism had been firmly established in political thinking by the turn of the 20th century. See Adrian Guelke, *The Age of Terrorism and the International Political System* (London: St. Martin's Press, 1995), 3.
6. Note that the term's origin in the French Revolution deviates from this general rule; in this case, terror was inflicted by a new revolutionary government, and other examples of government-inflicted terror campaigns can be found. The definition of terrorism has generated its own extensive literature, and it is not this author's intention to discuss or define the term further. See Guelke, 1-7; and Bard E. O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare* (New York: Brassey's, 1990), 13.
7. For example, only 20 percent of terrorist actions during the 1980s killed anyone, but those that did, killed more people as time passed. See Bruce Hoffman, *Terrorist Targeting: Tactics, Trends and Potentialities* (Santa Monica, CA: Rand, 1992), 3.
8. "But for all their bombings, terrorists thus far have seldom used explosives in ways calculated to kill great numbers of any civilian population." Brian M. Jenkins, "International Terrorism: Trends and Potentialities" in Alan D. Buckley and Daniel D. Olson, *International Terrorism: Current Research and Future Directions* (New Jersey: Avery, 1980), 105. Bombings constituted 50 percent of terrorist attacks between 1968 and 1992, a trend that has continued to the present day. See Hoffman, 2. Note that aircraft bombings, such as that at Lockerbie in 1988, provide some notable exceptions to this trend.
9. Hijackings generated most hostage-siege situations and constituted 33 percent of international terrorist incidents by the late 1960s. This had declined to 4 percent by the 1980s. This decline is largely attributed to security improvements and establishing dedicated crisis management capabilities. See Hoffman, 13.
10. Bruce Hoffman, *Responding to Terrorism Across the Technological Spectrum* (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994), 5.
11. Although the Brighton attack caused relatively few casualties, the sophisticated long-delay, structural attack device used was clearly intended to kill a large number of people.
12. Huntington foretells that "The fault lines between civilizations will be the battle lines of the future" and identifies the Islamic and Western Christian as two of the modern civilizations between which those fault lines will appear. Samuel P. Huntington, "The Clash of Civilizations?" *Foreign Affairs* (Summer 1993), 22.
13. See the discussion on negotiation in Hugh Smith, "International Terrorism: A Political Analysis" in *The Year Book of World Affairs 1977* (London: Steven & Sons, 1977), 142-46.
14. In the United States, consequence management measures are being developed under the federally mandated Nunn-Lugar-Domenici Domestic Preparedness Program. See "Defense Against Weapons of Mass Destruction Act," in the National Defense Authorization Act for Fiscal Year 1997 (Washington, DC: U.S. Government Printing Office [GPO], 23 September 1996), Title XIV of Public Law 104-201.
15. For example, the Australian government's National Anti-Terrorist Plan is, in U.S. terminology, a counterterrorist crisis management contingency plan, <http://www.sac-pav.gov.au/pscc/natp.html>, accessed November 2001.
16. For an insight into the world of elite counterterrorism, see Neil C. Livingstone, *The Cult of Counterterrorism* (Lexington, MA: Lexington Books, 1990).
17. In the United States, the Nunn-Lugar-Domenici Domestic Preparedness Program is aimed at developing a national consequence management capability for CBRNE attacks. See Title XIV, Public Law 104-201.
18. For an example of this capacity, see Bruce Hoffman's explanation of the Provisional Irish Republican Army's development of counter-countermeasures for British countermeasures in Northern Ireland in Hoffman, *Responding to Terrorism Across the Technological Spectrum*, 14-16.
19. For example, the Aleph (formerly Aum Shinrikyo) sect's 1995 sarin gas attack on the Tokyo subway system began with research into producing chemical and biological agents in 1992. *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo*, Staff Statement by the Senate Government Affairs Permanent Subcommittee on Investigations, 31 October 1995, at <http://www.fas.org/irp/congress/1995_rpt/aum/part04.htm>, accessed November 2001.
20. The 1998 bombings of the U.S. Embassies in East Africa provide a useful example of this type of long-term planning. See Judy Aita, "Bombing Trial Witness Describes Nairobi Surveillance Mission" *Middle East News Online*, 23 February 2001, at <http://www.middleeastwire.com/unitedstates/stories/20010223_meno.shtml>, accessed November 2001.
21. Another prompt U.S. government response was diverting all inbound international flights and grounding all civil aviation within the continental United States. Civil aviation remained heavily restricted while airport security procedures were enhanced. While sensible measures, these significantly affected U.S. business and Americans' way of life, magnifying the effect of the initial terrorist strikes. An interesting sequel is the nationwide grounding of Greyhound bus services after a nonterrorist attack on a driver.
22. This observation does not dismiss the posttraumatic stress disorder casualties that will certainly emerge nor the rescue workers who may subsequently develop illnesses related to environmental hazards at the incident sites.
23. Although prompted by the bombings on the U.S. Embassies in Tanzania and Kenya, the 1998 strikes against al-Qaeda sites in Sudan and Afghanistan could fit into this category.
24. The CBRNE response capabilities being developed in the United States under the Nunn-Lugar-Domenici Domestic Preparedness Program are an example of this.
25. These programs may also be the best means of addressing the clash of civilizations dimension in modern terrorist ideologies.
26. These problems have been identified in the United States, and efforts to address them have been the subject of Congressional scrutiny for several years. A lack of coordinated management may be one reason why President George W. Bush established a new Cabinet portfolio for homeland security. See testimony by Richard Davis, director, National Security Analysis, National Security and International Affairs Division (NSAID), U.S. General Accounting Office (USGAO) before the Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight, U.S. House of Representatives, 23 April 1998, GAO/T-NSIAD-98-164 in *Combating Terrorism: Observations on Crosscutting*, 3. See also testimony by Henry L. Hinton, Jr., Assistant Comptroller General, NSAID, USGAO, before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives, GAO/T-NSIAD-99-107, *Combating Terrorism: Observations on Federal Spending to Combat Terrorism*, 14.

Lieutenant Colonel Andrew J. Smith, Australian Army, is the Australian exchange instructor to the Department of Joint and Multinational Operations, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas. He received a B.A. from the Royal Military College, a graduate diploma in Defence Studies from Deakin University, and a master's degree from the University of New South Wales. He is a Ph.D. candidate in the Department of Politics, University College, Australian Defence Force Academy. His command and staff positions include serving with the United Nations Mine Clearance Training Team, Pakistan; and forming and commanding the Australian Defence Force's Joint Incident Response Unit that supported the 2000 Olympic Games in Sydney. His article "How Sharp a Sword: Defining Legitimacy in Offensive Capabilities" appeared in the September-October 1998 edition of The Australian Defence Force Journal.